ABSTRACT

Zero-knowledge authentication proves identity without revealing information about a secret that is used to prove that identity. An authentication agent performs authentication of a prover agent without knowledge or transfer of the secret. A non-centralized zero-knowledge authentication system contains multiple authentication agents, for access by multiple computers seeking access on a computer network through local prover agents. Once authenticated, those multiple computers may also implement authentication agents. The secret may periodically expire by publishing a new encrypted secret by a trusted source, thwarting attempts to factor or guess information about the secret.